International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 10 | Oct 2018 www.irjet.net p-ISSN: 2395-0072

Securing Cloud Data Under Key Exposure

S.Delfin[1], P. Abhilash Reddy[2], P.J. Surya Sankar Reddy[3],G. Sai Prudhvi[4]

[1,2,3,4]*Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram Campus, Chennai-89, INDIA.*

Abstract - *Cloud storage in public systems has become a major issue to control data access. A pliable and most secure way to secure the data in the cloud severs for cloud storage is by using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). But, in existing scheme the secure key distribution and verification is done by a single attribute authority which take a lot of time. When it is done by the single attribute authority, it is like a single-point play acquired in a big cloud storage system. There will be users who will be waiting for secret keys for a long-time which result in the less efficiency of the system. Many solutions have been proposed like multi authority scheme to overcome this problem but was unable to overcome this problem. So, in this paper we propose a new way to overcome this problem by using auditing mechanism. Auditing mechanism is like employing multiple attribute authorities to share the work in providing secret keys to the users who have been waiting for long time in queues. In this paper, the generation of keys is done by the Central authority for verified users. In this each authority is managed by the attribute individually. To improve the security of the process we also propose a mechanism which can detect the incorrectly verification process. Analysis shows that this process has great impact on the cloud security and its performance is better.*

Keywords: **Cloud storage, Security, CP-ABE, Auditing Mechanism, Single-point reference**.

1. INTRODUCTION

Cloud computing is a type of internet computing where the data is shared virtually among a pool of servers. People place lots of information in the cloud. The data which is placed in the cloud will have no physical possession by the users. Hence, cloud security becomes important for keeping the file safe in the cloud. Securing cloud data from unknown threats is a complicated as well as challenging task. There will be users who will be waiting for secret keys for a long-time which result in the less efficiency of the system. Among the proposed schemes the most efficient and secure way to secure the cloud data in cloud data storage systems is by using Ciphertext Policy Attribute Based Encryption. One of the major features of this scheme is that it allows the owners of the data to have complete controls over the file like providing permissions, accessing policies etc. Cryptography is using in this scheme to have access control over the cloud data. In this, the data is encrypted by using a special technique. The data is encrypted over the attributes with an access structure and a secret passcode is stamped on owner attributes. The user can only decrypt the file if the secret passcode linked with the attributes matches the passcode entered by the user. In this paper, the generation of keys is done by the Central authority for verified users. In this each authority is managed by the attribute individually. To improve the security of the process we also propose a mechanism which can detect the incorrectly verification process.

2. EXISTING SYSTEM

Cloud Computing is an internet-based computing which helps users share the files online by using internet. People place lots of information in the cloud. The data which is placed in the cloud will have no physical possession by the users. Hence, cloud security becomes important for keeping the file safe in the cloud. Securing cloud data from unknown threats is a complicated as well as challenging task. This makes the data protection in cloud a major problem. This paper ensures the integrity of the cloud data and security of the data stored in the cloud. In this paper, the data is stamped before uploading it to cloud. By using cloud services, users can gain access to their file remotely and can download it without having the need for storing data locally in the drives. Cloud computing ensures the integrity of the cloud data. Enabling the public auditability is of great need for users to be free from worries. The Third part auditors will check the integrity of the data and help the users for storing their data in the cloud happily. The Third-Party Auditors will bring no extra burden for the system and therefore helps for securing the data in the cloud at no additional cost. Analysis of the proposed system shows that the proposed system is not only intelligent but also secure and efficient.

3. PROPOSED SYSTEM

Server model or client model are not worthy for cloud storage devices. Thus, the challenging issue in the cloud data storage is the data access control. To overcome this

problem many schemes have been proposed worldwide. Among the proposed schemes the most efficient and secure way to secure the cloud data in cloud data storage systems is by using Ciphertext Policy Attribute Based Encryption. One of the major features of this scheme is that it allows the owners of the data to have complete controls over the file like providing permissions, accessing policies etc. Cryptography is using in this scheme to have access control over the cloud data. In this, the data is encrypted by using a special technique. The data is encrypted over the attributes with an access structure and a secret passcode is stamped on owner attributes. The user can only decrypt the file if the secret passcode linked with the attributes matches the passcode entered by the user. This scheme is evolved into two categories. They are single attribute authority and multiple attribute authority. In the single attribute authority there will be only one authority and in the multiple attribute authorities there will be more than two attribute authorities.

4. ARCHITECTURE DIAGRAM

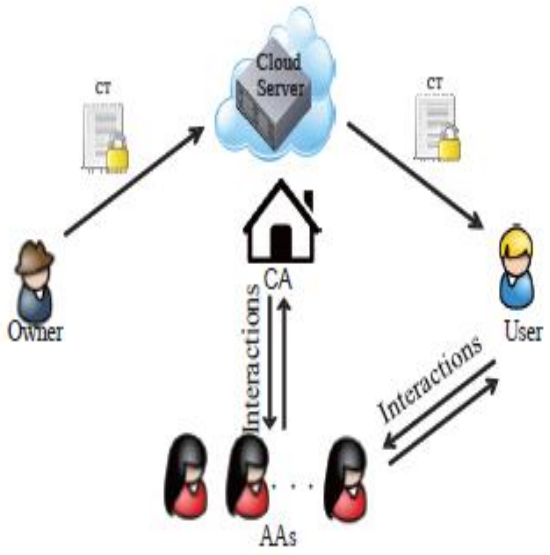

Fig -1:Architecture Diagram

5. LITERATURE SURVEY

In the software development procedure, literature survey is the most important step. It is important for us to decide the importance of the particular tool to shape the strength of the product. Once the importance of the thing is known, then the next step is the operating system and the language to use to complete the program. There should be much support for the coders while building a project. In the literature survey we found the various ways to secure cloud data. To secure a cloud data, the data owner must encrypt the file or the document before he uploads it to the cloud. The encrypted key is shared only with the users who request for the secret key. It is also needed to make sure that no two users will get the same passcode. After the user is provided with the passcode, the user will have access to view the file or download the file. This scheme increases the reliability of the users to send their data without hesitation.

6. ALGORITHMS USED

6.1 Clustering Algorithm

Clustering or cluster analysis is the way of clubbing a set of objects in such a way that the set of objects in similar set are more similar than the set of objects in other set. This is known as clustering algorithm.

6.2 Ciphertext-Policy Attribute-Based Encryption:

This algorithm encrypts the data uploaded by the owner and sets a passcode to it. Only the user with the passcodes can gain access to the file.

7. MODULE DESCRIPTION

1. User Module
2. Owner Module
3. Attribute authority Module
4. Central authority Module
5. Chart Module

7.1 User Module:

The data consumer (User) is assigned a global user identity by *CA*. The user possesses a set of attributes and is equipped with a secret key associated with his/her attribute set. The encrypted data in the cloud can freely be used by the user. The user can view the encrypted data only if the passcodes generated by the attribute authority matches the passcode entered by the user.

7.2 Owner module

The data owner (Owner) defines the access policy about who can get access to each file and encrypts the file under the defined policy. First of all, each owner encrypts his/her data with a symmetric encryption algorithm. The access policy is formulated by the owner and the owner encrypts the symmetric key following the policy and public key obtained by the central authority. After the symmetric key is encrypted the owner will send the whole data to the cloud central authority.

7.3 Admin module

Admin is a super user. they can view all the user and owner details, admin can view the chart based on most number of word search , they can add related word ,so user can easily mapping a related words for example Ambiguity level 2 refers to instances that most people think as ambiguous. These instances contain two or more unrelated senses, such as “apple” (fruit & company) and “jaguar” (animal & company). In this work, we only focus on instances that are disambiguous.

7.4 Attribute Authority module

The attribute authority is responsible for verifying the users by using the passcodes they enter for verification. After the verification is done by the attribute authority, the user gains access to view the file. In many of the multiple attribute authority schemes, the Attribute authority controls the disjoint attribute set separately. But, in the proposed system multiple attribute authorities share the work to increase the efficiency of the work.

In this the work is done individually. When an attribute authority is selected, it will verify the users attributes by manual labour or authentication protocols, and generate an intermediate key associated with the attributes that it has verified. Intermediate key is a new concept to assist central authority to generate keys.

7.5 Central Authority module

The central authority is the administrator of the entire system. It is responsible for the system construction by setting up the system parameters and generating public key for each attribute of the universal attribute set. In the initial stage, it assigns each user a separate ID and each AA a separate ID. For a key request from a user, Central authority holds responsibility for issuing passcodes for the user on the basis of the received intermediate key linked with the user’s attributes checked by an Attribute authority.

As central authority is the administrator of the whole system, he has the ability to trace which attribute authority has falsely verified a user and has issued the passcodes. The cloud server provides a public platform for owners to store and share their encrypted data. Data access control for the users is not provided by the cloud server. Any encrypted data in the cloud can be freely downloaded by the used after successful verification.

7.6 Chart module

chart module, chart module based on number of file download in particular user ,central authority can easily find out which file is downloaded more.

Table -1: Software Requirements

Operating System	Windows
Technology	Java and J2EE
Web Technologies	Html, JavaScript, CSS
IDE	My Eclipse
Web Server	Tomcat
Database	My SQL
Java Version	J2SDK1.8

Table -2: Hardware Requirements

Hardware	Pentium
Speed	1.1 GHz
RAM	1GB
Hard Disk	20 GB
Monitor	SVGA

8.Activity Diagrams

8.1 User

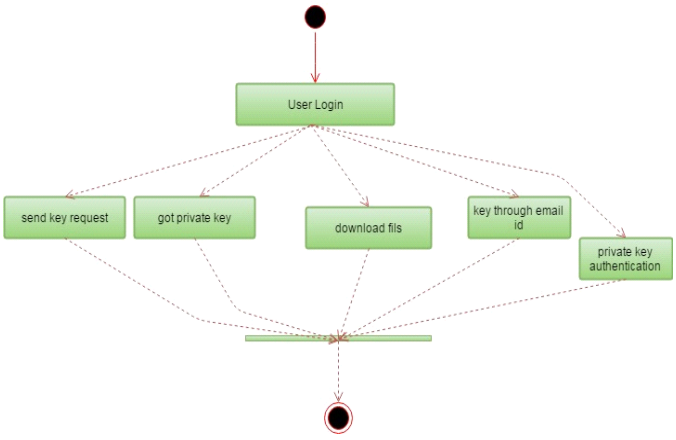

Fig -2: Activity Diagram of the user

8.2 Owner

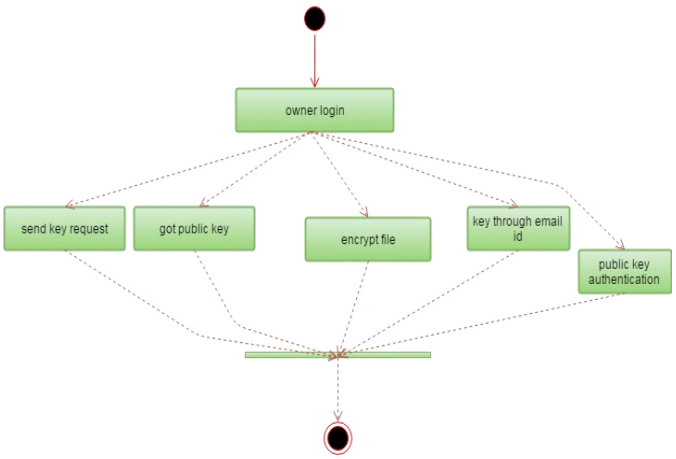

Fig -3: Activity Diagram of the owner

9. CONCLUSION

In this paper, we proposed a new method to overcome single point reference. The existing CP-ABE scheme is of single point reference and cannot ensure the integrity of the cloud data. By redesigning the current CP-ABE scheme from single attribute to multiple attribute authority, the process not only increased the efficiency of the system but also the user experience. By using this technique, the owner can have access control over the cloud data he uploads. This overcomes the problem of time taking verification and in our system for the owner to have the ability to upload a file he should have the passcode to gain the access to upload a file. After the file is uploaded, it is encrypted with passcodes. The user who wishes to view the file should request the attribute authority for passcodes. After the attribute authority accepts the request the user gets a passcode and enters in the website to view the file. The system validates the passcode entered by the user and if it matches the generated passcode then the user is allowed to view or download the file.

10. FUTURE ENHANCEMENT

The future enhancement for this CP-ABE process is that it can be made to find the malicious files and the owners who upload them. To track a person who uploads the files. To track the details of the members who downloaded a particular fiew and to see how many times a person viewed a particular file.

REFERENCES

[1]AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033- 3037, May-Jun 2012.

[2] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.

[3] Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii International Conference on System Sciences, pp.1-7, 2011.

[4] Kevin Curran, Sean Carlin and Mervyn Adams, "Security issues in cloud computing", Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.

[5] Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847),Volume 3 Issue 3, pp.171-176, March 2014.

[6] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering, Volume I, ISBN: 978-988-19251-3-8; ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) , 2012.

[7] Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3 Issue 5, pp.571-575, May 2013.

[8] L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security & Privacy Magazine, vol. 7, pp. 61-64, July2009.

[9] S C Rachana, Dr. H S Guruprasad, "Emerging Security Challenges in Cloud Computing ", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3 Issue 2, pp.485-490, March 2014.

[10] G. Devi , M. Pramod Kumar, "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803, pp. 592-596,2012.

[11] Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.

[12] Wayne Jansen ,Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication,NIST SP - 800- 144 ,80 pp., 2011.

[13] G. Lin, D. Fu, J. Zhu, and G. Dasmalchi, "Cloud Computing: IT asa Service," IT Professional, vol. 11, pp. 10-13, Mar./Apr.2009.

[14] Mandeep Kaur and Manish Mahajan, "Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology, Vol. 2, pp.831-835, October 2012.

[15] Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 3, pp.1922-1926, Jul-Aug 2013.

[16] Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , "Cloud Computing System Based on Trusted Computing Platform", International Conference on Intelligent Computation Technology and Automation, Volume 1, pp.942-945, 2010.

[17] Pearson, S., Benameur, A., Privacy, "Security and Trust Issues Arises from Cloud Computing", Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference, pp.693-702, 2010.

[18] Lizhe Wang, Gregor von Laszewski, Marcel Kunze, Jie Tao, Cheng Fu, Xi He, Andrew Younge, "Cloud Computing: A Perspective Study", New Generation Computing-Advances of Distributed Information Processing, Volume 28, pp.137-146, 2010.

[19] Puneet Jai Kaur, Sakshi Kaushal, "Security Concerns in Cloud Computing", Communication in Computer and Information Science Volume 169, pp.103-112, 2011.

[20] Priyanka Arora, Arun Singh, Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal, pp.179-183, 2012.